CONN LAW, PC
ELLIOT CONN Bar No. 279920
elliot@connlawpc.com
354 Pine Street, 5th Floor
San Francisco, CA 94104
Telephone: (415) 417-2780
Facsimile: (415) 358-4941

ADELPHI LAW
JOSHUA WHITAKER (*admitted pro hac vice*)
whitaker@adelphilaw.com
2306 Wineberry Terrace
Baltimore, MD 21209
Telephone: (888) 367-0383
Facsimile: (888) 367-0383

Attorneys for Plaintiffs Hadona Diep, Ryumei Nagao, and the putative class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

HADONA DIEP and RYUMEI NAGAO, individually, on behalf of all others similarly situated, and on behalf of the general public

Plaintiffs.

vs.

APPLE, INC.,

Defendant.
_____/

Case No. 4:21-cv-10063-PJH

PLAINTIFFS' OPPOSITION TO DEFENDANT APPLE, INC.'S MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

Judge: Hon. Phyllis J. Hamilton
Date: August 4, 2022
Time: 1:30 p.m.
Courtroom: 3
Trial Date: N/A

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes & Rules

I. INTRODUCTION

Plaintiffs Hadona Diep and Ryumei Nagao, like millions (if not billions) of other consumers, have been exposed to a decades-long advertising campaign by Defendant Apple, Inc. that touts the absolute "safety and security" of Apple's products. With respect to the applications (colloquially, "apps") that Apple makes available in its App Store, Apple explicitly represents that "the apps we offer are held to the highest standards for privacy, security, and content. Because we offer nearly two million apps — and we want you to feel good about using every single one of them."

Reasonably relying on the guarantee that the App Store is "a safe and trusted place," Plaintiffs both downloaded what they believed to be a legitimate cryptocurrency wallet, the "Toast Plus" app and transferred substantial amounts of cryptocurrency to their wallets. Unfortunately, Apple's representations of "safety and security" have proved inaccurate, and the "Toast Plus" app was actually a "spoofing" / "phishing" program that was designed solely to steal Plaintiffs' (and other consumers') cryptocurrency. This lawsuit was only brought after Apple refused to take any responsibility for the damages suffered by Plaintiffs after relying upon Apple's safety and security representations.

In a further attempt to evade accountability, Apple has brought a Motion to Dismiss that misstates the underlying allegations, the claims asserted, and the relevant case law.
But Apple cannot so easily evade liability for the substantial losses suffered by Plaintiffs, and the putative class, in reliance on Apple's own misrepresentations of "safety." Each of the causes of action asserted are adequately pled, and for the reasons set forth herein, Apple's Motion should be denied.

II. RELEVANT ALLEGATIONS

The operative First Amended Complaint ("FAC") alleges that Apple has engaged in a long-standing campaign of representing that its App Store is "a safe and trusted place" and that Apple "[ensures] that the apps we offer are held to the highest standards for privacy, security, and content. Because we offer nearly two million apps — and we want you to feel good about using every single one of them." (Dkt. 33, First Amended Complaint ("FAC"), ¶¶ 2, 14-17).

Apple controls what apps may be sold or provided to consumers through the App Store by a rigorous vetting process that involves provision of the proposed apps' purpose and a copy of the app itself and any relevant source code, users' guides, and software documentation.[1] (*Id.* ¶ 18). And Apple customers have no other practical or convenient manner in which to download applications for their iPhones or iPads, as Apple maintains rigorous control over applications that can be placed on their devices. (*Id*. ¶ 19). *see also* Mot. at 4:13-16 (representing that "[a]ll apps on the App Store are subject to, and must comply with, [ ] guidelines to 'address issues of safety, privacy, performance, and reliability' of all apps made available through the App Store.) (quoting *Epic Games, Inc. v. Apple, Inc.*, No. 4:20-cv-05640, 2021 WL 4128925 (N.D. Cal. Sept. 10, 2021)).

Through its long-standing campaign of intentional and deliberate representations touting that the App Store is a "safe and trusted place," Apple induced Plaintiffs and the putative class, to trust the products that were offered in the App Store, and in reliance on Apple's representations, that trusted and downloaded the Toast Plus app, causing them to lose their cryptocurrency to thieves. (FAC, ¶ 2).

Apple knew or should have known of the fraudulent purpose of the Toast Plus app, and failed to take remedial action, causing harm to the Plaintiffs and the Class. (*Id*. ¶ 2). In fact, Apple knew of the true fraudulent purpose of the Toast Plus app before allowing it to be distributed on the App Store, since Apple "vetted" the application prior to allowing it to be distributed on the App Store, or, alternatively, came to know of the Toast Plus app's true purpose soon after distributing it. (*Id.* ¶¶ 18, 50-51). Apple also allowed the application developer in this case to use a name and logo of a legitimate cryptocurrency wallet provider, Toast Wallet, thereby misleading Plaintiffs and reinforcing Apple's misrepresentations as to safety and security. (*Id.* ¶ 23).

Based on the concrete monetary losses sustained (and Apple's refusal to take any responsibility), Plaintiffs have brought claims on their own behalf and on behalf of similarly-

[1] If necessary, Plaintiffs can amend the Complaint to provided more detailed allegations as to Apple's direct involvement in the creation of the apps it provides.

situated persons against Apple, Inc., for violations of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030, *et seq.* (Count I) ("CFAA"), violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.* (Count II) ("ECPA"), violations of the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100, *et seq*. (Count III) ("CCPA"), violations of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (Count IV) ("UCL"), violations of the Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (Count V) ("CLRA"), interception and disclosure of electronic communications in violation of Maryland Code, Wiretap & Electronic Surveillance Act § 10-402(a) (Counts VI & VII), violation(s) of the Maryland Personal Information Protection Act, Maryland Annotated Code, Commercial Law, § 14-3501, *et seq.* (Count VIII) ("PIPA"), violation(s) of the Maryland Consumer Protection Act, Maryland Code, Code, Commercial Law, § 13-101, *et seq*. (Count IX) ("MCPA"), and negligence (Count X), related to Apple's part in authorizing and negligently distributing a "phishing" / "spoofing" app in its App Store, the "Toast Plus" application, while continuing to affirmatively represent that the App Store is a "a safe and trust[ed] place."

III. LEGAL STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), the Court is required to accept as true all factual allegations set forth in the complaint, as well as all reasonable inferences to be drawn from them. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007); *Cahill v. Liberty Mutual Ins. Co.*, 80 F.3d 336, 338 (9th Cir. 1996). A well-pleaded complaint need only set forth a short and plain statement of the claim showing that the pleader is plausibly entitled to relief. Fed. R. Civ. Proc. 8(a)(2); *Twombly*, *supra*, at 555. As the Supreme Court has explained, showing plausible grounds for recovery does not require a showing that recovery is probable. *Id.* at 556.

A motion to dismiss challenges only the legal sufficiency of the complaint. Dismissal is proper only where insufficient facts are alleged to support a cognizable legal theory. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). A complaint should not be dismissed unless a plaintiff can prove no set of facts in support of their claim which would entitle them to relief. *Cahill, supra*, 80 F.3d at 339. In reviewing the allegations, the Court is required to construe the complaint "with the utmost liberality" to determine whether a cause of action has been stated.

Fed. R. Civ. Proc. 8(f); *Yamaguchi v. U.S. Dept. of the Air Force*, 109 F.3d 1475, 1480-81 (9th Cir. 1997).

IV. ISSUES TO BE DECIDED

1. Does "Online Publisher" immunity under the Communications Decency Act immunize Apple for its own misrepresentations?
2. At the Motion to Dismiss stage, can Apple use extrinsic evidence "Terms" to prospectively waive consumers' rights under un-waivable State and Federal statutes?
3. Are Japanese residents *per se* prevented from suing Apple for Apple's unfair and deceptive acts and practices?
4. Can Apple customers who have lost identifiable sums of money in reasonable reliance on Apple's misrepresentations regarding the "safety and security" of Apple's products seek recourse against Apple under State and Federal statutes and common law claims, including the CFAA, CCPA, UCL, CLRA, Wiretap Acts, PIPA, MCPA, and negligence?

V. LEGAL ARGUMENT

A. The Communications Decency Act Does Not Immunize Apple for its Own Misrepresentations

As noted above, Plaintiffs, in the First Amended Complaint, largely allege not that Apple was acting as a publisher of other's content, but, rather, that Apple must be held liable for its own misrepresentations as to the safety and security of the apps in the App Store.

Plaintiffs' UCL (Count IV), CLRA (Count V), MCPA (Count IX), and Negligence (Count X) claims are all predicated *solely* on Apple's own misrepresentations. (FAC, ¶¶ 93-95, 102-103, 147-149, 155). Communication Decency Act ("CDA"), 47 U.S.C. § 230(c)(1) "immunity" does not apply if Apple "created or developed the particular information at issue." *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1125 (9th Cir. 2003).

Courts in this district have rejected the exact theory that Apple brings here. In *Pirozzi v. Apple, Inc.*, 913 F.Supp.2d 840 (N.D. Cal. 2012), the Honorable Yvonne Gonzalez Rogers rejected the argument that Apple re-raises here, noting that:

> Apple's arguments, however, misconstrue the nature of certain of the allegations in the CAC. Plaintiff's claims are not predicated solely upon Apple's approving and distributing Apps via its online App Store; Plaintiff also seeks to hold Apple liable for representations made by Apple itself. As Apple acknowledges, Plaintiff's claims include "allegations that Apple somehow misled Plaintiff as to the 'nature and integrity of Apple's products.'" To the extent that Plaintiff's claims allege that Apple's misrepresentations induced Plaintiff to purchase an Apple Device, those claims do not seek to hold Apple liable for making Apps available on its website. In that context, even if Apple acts as an "interactive computer service," Plaintiff seeks to hold it liable as the "information content provider" for the statements at issue.

Id. at 849.

Consistent with Judge Gonzalez Rogers' ruling, in other litigation in this judicial district, Apple has accepted that reasoning to be correct. For example, it did not challenge the misrepresentation claims in *Opperman v. Path, Inc*., 87 F.Supp.3d 1018, 1044 (N.D. Cal. 2014) ("Apple expressly excludes from its CDA argument any application to Plaintiffs' fraud and misrepresentation claims, in recognition of Judge Gonzalez Rogers' first conclusion.").

Despite this, here, Apple deliberately misconstrues the allegations in the FAC, and focuses instead on the application review process and the fact that Toast Plus was created by a third-party. *See, generally*, Mot. at 5-8.

But this is not what the Plaintiffs have complained of. As noted above, Plaintiffs were misled by Apple's own published statements as to the App Store being a "safe and trusted place to discover and download apps," by Apple stating that it ensures "that the apps we offer are held to the highest standards for privacy, security, and content," and that Apple wants users "to feel good about using every single one of [of the millions of applications on the App Store]." (FAC, ¶ 14) (citing to App Store website); *see also* Mot. at 4:13-16 (recognizing that "[a]ll apps on the App Store are subject to, and must comply with, [ ] guidelines to 'address issues of safety, privacy, performance, and reliability' of all apps made available through the App Store.") (quoting *Epic Games, Inc.*, 2021 WL 4128925).

Apple cannot deny that it is the author of its own corporate marketing statements. This is not a CDA issue - it is only because of Apple's false or negligent representations that Plaintiffs downloaded and used the Toast Plus app in the first place. (FAC, ¶ 2) (stating that Plaintiffs,

"relying on Apple's express representations that its Apps were safe, Plaintiffs and Class Members transferred cryptocurrency to Toast Plus, which was subsequently stolen.").

Plaintiffs' claims are based on Apple's own statements. In fact, even in its own Motion, Apple continues to represent that it holds the App Store out as being a place of security and privacy. Mot. at 4:13-16. The CDA therefore does not provide it with immunity.[2]

And at this stage, Plaintiffs do not concede that Apple was not responsible in any part for the creation of the Toast Plus app. Based on the pending Motion, Apple has objected to providing even initial disclosures. While Plaintiffs have made allegations regarding Apple's overall "vetting" process, discovery here will show exactly what specific changes to the code and assistance that Apple gave the "Toast Plus" developers, which will allow the Court to make a determination with a full record as to whether Apple is "content creator" for the purposes of the CDA. At this time, making such a determination would be premature. *See Pirozzi*, 913 F.Supp.2d at 849 (stating that, "based on the scant record before the Court, it is premature to decide whether the CDA bars Plaintiff's claims . . . if Apple is responsible for the 'creation or development of [the] information' at issue, then Apple functions as an 'information content provider' unprotected by the CDA.") (quoting *Carafano*, 339 F.3d at 1124-25).

But regardless of whether Apple is a "publisher," the CDA has "[n]o effect on criminal law" and does not "impair the enforcement of . . . any other Federal criminal statute." 47 U.S.C. § 230(e)(1). Similar, the CDA has "[n]o effect on communications privacy law" and does not "limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law." 47 U.S.C. § 230(e)(4). By the express terms of the statute itself, the CDA does not give Apple immunity for its violations of the federal claims asserted (Counts I and II) or for its violations of the state law privacy claims (Counts III,

[2] It is well-established that representations made in advertising campaigns can be the basis of liability for the publisher, even when a claimant does not have the ability to point to a particular advertisement that she or he saw. *See In re Tobacco II Cases*, 46 Cal.4th 298, 328 (2009) ("where, as here, a plaintiff alleges exposure to a long-term advertising campaign, the plaintiff is not required to plead with an unrealistic degree of specificity that the plaintiff relied on particular advertisements or statements"). (*see also* FAC, ¶¶ 16, 17).

VI, VII, VIII). And given that the remaining claims focus entirely on Apple's own statements, the CDA provides Apple with no defense whatsoever.

B. California Law Prohibits the Prospective Waiver of the Claims Asserted

The extrinsic evidence provided by Apple via the proffered "Terms" also has no impact on Plaintiffs' claims. In fact, Apple, a California company, recognizes that its "limitation of liability" provision is limited "TO THE EXTENT NOT PROHIBITED BY LAW" (Dkt. 43-3, 43-4, Terms § G(f)).

Such a "prohibition" applies in full force under the substantive law of California, which provides that "a law established for a public reason cannot be contravened by a private agreement" (Cal. Civ. Code § 3513) and that "[a]ll contracts which have for their object, directly or indirectly, to exempt any one from responsibility for his own fraud, or willful injury to the person or property of another, *or violation of law*, whether willful or negligent, *are against the policy of the law*." (Cal. Civ. Code § 1668) (emphasis added). *See also Health Net of California, Inc. v. Dep't of Health Servs.*, 113 Cal.App.4th 224, 235 (2003) (surveying cases, finding that "California courts have construed [Civil Code § 1668] for more than 85 years to at least invalidate contract clauses that relieve a party from responsibility for future statutory and regulatory violations.").

Consistent with this, each of the civil statutory claims asserted are "unwaivable." *See* Cal. Civ. Code § 1798.192 (waiver of rights under the California Consumer Privacy Act are "shall be deemed contrary to public policy and shall be void and unenforceable."); Cal. Civ. Code § 1751 ("Any waiver by a consumer of the provisions of [the Consumers Legal Remedies Act] is contrary to public policy and shall be unenforceable and void."); *McGill v. Citibank, N.A.*, 2 Cal.5th 945, 961 (2017) (finding waiver of CLRA and Unfair Competition law public injunctive claims "invalid and unenforceable under California law."); Md. Code Ann., Comm. Law Art. § 13-103(a) (Maryland Consumer Protection Act "is intended to provide minimum standards for the protection of consumers in the State.").

Similarly, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq*., and the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*., are both contained within

U.S.C. Title 18, "Crimes and Criminal Procedures" and as penal provision are laws established for a public reason cannot be waived. *W. Surgical Supply Co. v. Affleck*, 110 Cal.App.2d 388, 392 (1952).

Finally, it is well established that "California law forbids limiting liability for gross negligence." *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F.Supp.3d 767, 800 (N.D. Cal. 2019). And since "[o]rdinary and gross negligence are not separate causes of action in California . . . , the applicability of the waiver will turn at least in part on the degree of negligence (if any) that the plaintiffs can ultimately prove." *Id*. (citations omitted).

The cases cited by Apple do not hold differently. The cited opinion *In re Apple In-App Purchase Litig.*, 855 F.Supp.2d 1030, 1034 (N.D. Cal. 2012) did not make any substantive determination as to the enforceability of Apple's exculpatory clauses, it merely noted that "California substantive law applies to the instant case." In *Minkler v. Apple, Inc.*, 65 F.Supp.3d 810, 818, 821 (N.D. Cal. 2014), the court only looked at the terms of an express warranty and did not make any finding with respect to the "limitation of liability provision" proffered here.

And the court's holding in *Barrett v. Apple Inc.*, 523 F.Supp.3d 1132, 1153-55 (N.D. Cal. 2021) was based on a finding that the Plaintiffs had not alleged both prongs of unconscionability and thus the asserted claim for "unconscionability" was dismissed without prejudice. In so ruling, the court noted that there was no substantive unconscionability because, "[h]ere, Apple's disclaimer does not attempt to avoid California unfair competition statutes or otherwise contract around the law." *Barrett*, 523 F.Supp.3d at 1154–55. In contrast to the position taken in *Barrett*, here Apple is trying to use its "limitation of liability provision" "to avoid California unfair competition statutes." Regardless, Plaintiffs have not asserted a direct claim for "unconscionability." Thus, the holding in *Barrett*, and the remaining authority cited by Apple are inapposite. The Motion should be denied as to Apple's assertion of immunity based on its "Terms."

C. Plaintiff Nagao May Sue Apple for Its Unlawful Conduct

Just as Apple cannot use its "terms" to waive Plaintiffs' claims, it also does not get to decide who Plaintiffs sue. Here, Plaintiffs both allege that Apple, not its wholly owned

subsidiary, committed unfair and deceptive acts or omissions in violation of Federal, California and Maryland statutory law and common law negligence. Plaintiffs have alleged that it was Apple, not a Japanese subsidiary, that represented to the entire world that the App Store is a "safe and trusted place to discover and download apps." (FAC, ¶ 14). Plaintiff Nagao has alleged that it was Apple, not its wholly owned subsidiary, that failed "to properly vet the Toast Plus application before providing it to the public," that failed "to warn the public of the actual risks of applications in the App Store," that failed "to remove Toast Plus from the App Store after learning of its dangerous nature, and or by failing to warn or notify each Toast Plus user of the danger after learning of the danger itself." (*Id.* ¶ 2). Lastly, once learning of the fraud, Plaintiff Nagao contacted Apple, not its unknown subsidiary. (*Id*. ¶ 34).

This is at heart an Unfair Deceptive Acts and Practices case based upon Apple's tortious conduct, misrepresentations and/or negligence. Unlike most of the cases cited by Apple, Plaintiffs have not alleged "breach of contract."[3] Rather, Plaintiff Nagao alleges counts of unfair practices that violate Federal and California statutory law and constitute common law negligence against the party who committed the bad conduct – Apple. The Motion should be denied.

D. Plaintiffs Have Alleged Violation of the Computer Fraud and Abuse Act

Apple's argument as to Count I, the CFAA, ignores the actual allegations. As the Ninth Circuit has held, the CFAA "target[s] the unauthorized procurement or alteration of information[.]" *United States v. Nosal,* 676 F.3d 854, 863 (9th Cir. 2012) (quoting *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 965 (D.Ariz.2008)). Plaintiffs have alleged that the Toast Plus app is designed to exceed the authorization that users agree to because it is a "phishing" and "spoofing" app, (FAC, ¶ 50), and Apple knew of the fraudulent purpose of Toast Plus prior to allowing it to be distributed on the App Store because of its "rigorous vetting process." (*Id*. ¶¶ 18, 51).[4]

[3] Apple also cites to *Johnson v. Mammoth Recreations, Inc.*, 975 F.2d 604 (9th Cir. 1992), an opinion that addresses a summary judgment ruling that made a factual finding that the wrong party had been made. The opinion is inapposite at the motion to dismiss stage.

[4] "Phishing" that results in loss is an illegal act under CFAA. *United States v. Iyamu*, 356 F.Supp.3d 810, 814 (D. Minn. 2018)

Furthermore, this is not a case of users *authorizing* the conduct, rather, it is a case of *exceeding* the authorization that was given, because the app in question did not do what it purported to do, which Apple knew prior to distributing it to unknowing users. *See* fn. 4, *supra* (noting that "phishing" is a criminal violation of CFAA). Plaintiffs consented to downloading a cryptocurrency wallet, they did not consent to download a "spoofing" / "phishing" scam. *See San Miguel v. HP Inc.*, 317 F.Supp.3d 1075, 1086 (N.D. Cal. 2018) (upholding § 1030(a)(5)(A) claim against motion to dismiss where plaintiffs alleged they authorized software update, not that they authorized damage to their devices).

Since Apple knew that it would be distributing a "spoofing" / "phishing" app and did so anyways, it participated in the exceeding of authorization of access, and or conspired to do the same, by intentionally and overtly distributing the fraudulent Toast Plus app. FAC, ¶ 53. It is therefore odd that Apple argues that "there are no allegations that Apple intended to defraud," Mot. at 12:13, since the Plaintiffs alleged that the Toast Plus app, which Apple "vetted," had a "sole purpose [ ] to entice consumers to divulge their cryptocurrency account information, by mimicking an established cryptocurrency wallet in name, mark, and design, thereby allowing hackers to steal that cryptocurrency . . ." and that Apple knew of that fraudulent purpose "prior to authorizing it for distribution on the App Store." (FAC, ¶¶ 50-51); *c.f., Nowak v. Xapo, Inc.*, Case No. 5:20-cv-03643-BLF, 2020 WL 6822888, at *3 (N.D. Cal. Nov. 20, 2020) (claimant there did not plead defendant knew of the hacking, unlike the allegations here). Apple ignores that it was accused of conspiring with the Toast Plus developers (FAC, ¶ 53), in asserting that "Apple was not involved in Plaintiffs' interaction with the Toast Plus app." Mot. at 12:11-12.

Apple's arguments fail and the Motion should be denied as to Count I.

E. Plaintiffs Have Alleged Violations of the ECPA

As to the ECPA claim (Count II), Apple's argument ignores the crucial allegation that Plaintiffs downloaded the Toast Plus "spoofing" or "phishing" app *from Apple* and not from the unknown third-party developer of the fraud. (FAC, ¶¶ 2, 22). The unlawful interception and disclosure of Plaintiffs' seed phrases (*Id*. ¶¶ 25, 26, 27), occurred as a result of the seed phrase

being entered into the app and on Plaintiffs' Apple devices, which were then intercepted and disclosed. (*See also Id*. ¶¶ 62-67).

As it was the Apple app itself, which Apple had vetted, approved of, made available in the App Store, on its own servers, that intercepted and disclosed the communication, it was *Apple* that intercepted and disclosed the seed phrases. Apple was not the "means through which" a third-party intercepted a communication, it was Apple product itself that intercepted and disclosed the communication and sensitive information. And Apple's "intent" can be shown through the fact that the App went through a "rigorous vetting process," meaning Apple knew that it was published a fraud. (FAC, ¶ 18).

Apple's reliance on *United States v. Peterson*, 812 F.2d 486 (9th Cir. 1987) is misplaced. In *Peterson*, the Circuit Court considered Drug Enforcement Administration involvement in a Thai wiretapping operation required Title III of the Omnibus Crime Act compliance. Here, there is no allegation that Apple endeavored to do anything outside of the United States – in fact, the allegations in the First Amended Complaint are that Apple engaged in the relevant activities in California. (FAC, ¶ 11) (stating that "Defendant is located in this judicial district and/or a substantial part of the acts or omissions giving rise to the claims herein occurred in the same."). The Motion should be denied as to Count II.

F. Plaintiff Diep Has Alleged Violations of the Maryland Wiretap and Electronic Surveillance Act

Apple's argument as to the Maryland wiretapping statute fail for the same reason. Apple there also ignores that Plaintiff alleges that Apple "procured others to intercept or endeavor to intercept the 'contents' of Plaintiff Diep's and Maryland Subclass Members' internet communications, related records, subscriber identity, or other information, without authorization. . .", in violation of the Maryland wiretapping statute. (FAC, ¶ 120).

G. Plaintiffs Alleged Claims Under the Unfair Competition Law and Consumers Legal Remedies Act

California's CLRA and UCL form the cornerstone of California consumer protection. The CLRA, by statute, is to "be liberally construed and applied to promote its underlying

purposes, which are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection." Cal. Civ. Code § 1760. And the UCL "broadly prohibit unlawful, unfair, and fraudulent business acts." *Sybersound Recs., Inc. v. UAV Corp.*, 517 F.3d 1137, 1151 (9th Cir. 2008) (citing *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal.4th 1134, 1143 (2003)). In trying to argue that a class of consumers that have lost concrete sums of money in direct reliance on Apple's misrepresentations *cannot* bring claims under the CLRA or UCL, Apple attempts to turn these statutes on their heads. Contrary to Apple's assertions otherwise, Plaintiffs have alleged viable claims under both statutes:

1. Plaintiffs Have Satisfied Any "Heightened" Pleading Requirements

To state a claim under the fraud prong of the UCL, it is unnecessary to show the elements of common law fraud, only that "members of the public are likely to be deceived" by the practice. *In re Tobacco II Cases*, 46 Cal.4th 298, 312. "This distinction reflects the UCL's focus on the defendant's conduct, rather than the plaintiff's damages, in service of the statute's larger purpose of protecting the general public against unscrupulous business practices." *Id*.

The fraud prong is broad and covers cases where there is no "advertising" and where there is no affirmative or untrue statement:

> [A fraud prong claim] may be based on representations to the public which are untrue, and '"also those which may be accurate on some level, but will nonetheless tend to mislead or deceive. … *A perfectly true statement couched in such a manner that it is likely to mislead or deceive the consumer, such as by failure to disclose other relevant information, is actionable under"' the UCL.* The determination as to whether a business practice is deceptive is based on the likely effect such practice would have on a reasonable consumer."

Klein v. Chevron U.S.A., Inc., 202 Cal.App.4th 1342, 1380-1381 (2012), (emphasis added, internal citations omitted).

And "where, as here, a plaintiff alleges exposure to a long-term advertising campaign, the plaintiff is not required to plead with an unrealistic degree of specificity that the plaintiff relied on particular advertisements or statements." *In re Tobacco II Cases*, 46 Cal.4th at 328.

Plaintiffs' CLRA claim can be analyzed under the same standard. *Williams v. Gerber Prod. Co.*, 552 F.3d 934, 938 (9th Cir. 2008).

The First Amended Complaint satisfies this pleading standard: "Plaintiffs and Class Members relied on Apple's long-standing campaign of representing that its App Store is 'a safe and trusted place' and downloaded a 'Toast Plus' application to store cryptocurrency. Unknown to Plaintiffs and Class Members, in actuality, the Toast Plus application was a 'spoofing' or 'phishing' program created for the sole purpose of stealing cryptocurrency, by obtaining consumers' cryptocurrency account information and thereafter routing the same to the hackers' personal accounts. Not knowing this, and relying on Apple's express representations that its Apps were safe, Plaintiffs and Class Members transferred cryptocurrency to Toast Plus, which was subsequently stolen. And despite numerous complaints regarding the fraudulent nature of the Toast Plus application, Apple allowed it to remain in the App Store and failed to warn Plaintiffs and Class Members of the danger of the application . . ." (FAC, ¶ 2) and "The business acts, omissions, and practices alleged herein constitute fraudulent business practices in that said acts and practices are likely to deceive consumers as to their legal rights and obligations, and by use of such deception, may preclude such individuals from exercising legal rights to which they are entitled."

And Apple cannot avoid liability for its express misrepresentations of safety through prolix "disclaimers." At most, the hidden contrary statements raise a question of fact "of whether a reasonable consumer is likely to be deceived . . ." *Mullins v. Premier Nutrition Corp.*, 178 F.Supp.3d 867, 892 (N.D. Cal. 2016). Unlike the cases cited by Apple, "[t]he facts of this case . . . do not amount to the rare situation in which granting a motion to dismiss is appropriate." *Williams*, 552 F.3d at 939.[5]

[5] *Hoai Dang v. Samsung Elecs. Co.*, No. 14-CV-00530-LHK, 2018 WL 6308738, at *8 (N.D. Cal. Dec. 3, 2018), *aff'd*, 803 F.App'x 137 (9th Cir. 2020) (granting motion to dismiss where "Plaintiff cannot plausibly claim that a consumer would understand the brand name 'Samsung' on a package label to mean that the phone in that package included no parts infringing another's patent. Thus, the Court concludes that Plaintiff has again failed to allege a misrepresentation or omission under the CLRA."); *Girard v. Toyota Motor Sales, U.S.A., Inc.*, 316 F.App'x 561, 563 (9th Cir. 2008) (affirming granting of motion to dismiss where "[e]ach of the two-page documents at issue includes numerous eligibility disclaimers and recommendations to seek professional tax advice, which put readers on notice of hybrid tax credit restrictions."); *Gudgel v. Clorox Co.*, 514 F.Supp.3d 1177, 1186 (N.D. Cal. 2021) (granting motion dismiss in "rare situation" where "this case involves no actual misrepresentation or deception that conflicts with the language of the product's disclaimer that it is 'not for sanitization or disinfection.'")

2. Plaintiffs Have Identified Actionable Omissions

Plaintiffs have also identified actionable omissions. "[A]n omission is actionable under the CLRA if the omitted fact is (1) 'contrary to a [material] representation actually made by the defendant' or (2) is 'a fact the defendant was obliged to disclose.'" *Gutierrez v. Carmax Auto Superstores California*, 19 Cal.App.5th 1234, 1258 (2018), *as modified on denial of reh'g* (Feb. 22, 2018). "In the context of the CLRA, a fact is 'material' if a reasonable consumer would deem it important in determining how to act in the transaction at issue. [Citation.] In other words, a defendant has a duty to disclose when the fact is known to the defendant and the failure to disclose it is ''misleading in light of other facts ... that [the defendant] did disclose.' ' " *Id*.

Plaintiffs have alleged that "Apple controls what applications may be sold or provided to consumers through the App Store by a rigorous vetting process that involves provision of the proposed application's purpose and a copy of the application itself and any relevant source code, users' guides, and software documentation" (FAC, ¶ 18), that "despite numerous complaints regarding the fraudulent nature of the Toast Plus application, Apple allowed it to remain in the App Store and failed to warn Plaintiffs and Class Members of the danger of the application" (*Id*. ¶ 2), and "Apple failed to properly vet the Toast Plus application before providing it to the public, failed to warn the public of the actual risks of applications in the App Store, failed to remove Toast Plus from the App Store after learning of its dangerous nature, and failed to warn or notify each Toast Plus user of the danger after learning of the danger itself." (*Id*. ¶ 103).

Such allegations are sufficient at this stage to show "pre-sale knowledge."

3. Plaintiffs' Relationship with Apple Confers Standing Under the CLRA

Plaintiffs also have "standing" under the CLRA.

The term "transaction" is broadly defined to mean "an agreement between a consumer and another person, whether or not the agreement is a contract enforceable by action, and includes the making of, and the performance pursuant to, that agreement. Cal. Civ. Code § 1761(a). "Nothing in the language of the CLRA states that only a defendant who directly engaged in a completed transaction with a plaintiff may be liable to that plaintiff. Viewed in light

of the provision to construe the statute liberally, the broad language of the statute suggests that the legislature intended the CLRA to cover a wide range of business activities." *Chamberlan v. Ford Motor Co.*, No. C 03-2628 CW, 2003 WL 25751413, at *7 (N.D. Cal., Aug. 6, 2003).

As alleged in the First Amended Complaint, Plaintiffs ongoing relationships with Apple constitutes a "transaction." Plaintiffs' "transaction" with Apple goes beyond the mere download of the Toast Plus application, it includes their purchase and use of Apple devices (FAC, ¶¶ 12, 19, 21). "Accordingly, at the pleading stage, at least, Plaintiffs have sufficiently alleged that they are consumers under the CLRA, and their allegations relate to the purchase of goods." *In re iPhone Application Litig.*, 844 F.Supp.2d 1040, 1071 (N.D. Cal. 2012). If necessary, the operative Complaint can be amended to provide more detailed allegations regarding Plaintiffs' ongoing "transactions" with Apple.

4. Plaintiffs Have Alleged Unlawful and Unfair Conduct Under the UCL

By proscribing any "unlawful" business act or practice, the UCL "borrows" rules set out in other laws and makes violations of those rules independently actionable. *Zhang v. Superior Court*, 57 Cal.4th 364, 370 (2013). Plaintiffs have alleged that Apple has engaged in an unlawful business act or practice, including violating the CFAA, ECPA, and CLRA. (FAC, ¶¶ 48-76, 100-114). These predicate violations support the "unlawful" aspect of the UCL claim.

A business practice is "unfair" when it "offends an established public policy or is immoral, unethical, oppressive, unscrupulous, unconscionable or substantially injurious to consumers." *Kunert v. Mission Fin. Servs. Corp.*, 110 Cal.App.4th 242, 265 (2003) (citations omitted).

Apple has engaged in a long-standing campaign of representing that its App Store is "a safe and trusted place." Despite this, Apple has approved "spoofing" and "phishing" applications for download and despite numerous complaints regarding the fraudulent natures of such applications, has allowed them to remain in the App Store and failed to warn its customers of the danger of such applications. Apple also allowed the "phishing" / "spoofing" app to take a deceptively similar name, mark, logo, and appearance of a legitimate app, thereby confusing the consumer into downloading the wrong app. Such conduct is objectively unfair.

Plaintiffs' allegations also satisfy all three formulations of the unfair prong.

First, Plaintiffs explicitly allege that "[t]he business acts, omissions, and practices alleged herein constitute unfair business practices in that said acts and practices offend public policy and are substantially injurious to the public" (FAC, ¶ 91). Such allegations satisfy the FTC's 1964 unfairness standard[6] as adopted in *People v. Casa Blanca Convalescent Homes, Inc.*, 159 Cal.App.3d 509, 530 (1984).

Second, Plaintiffs satisfy the *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*, 20 Cal.4th 163, 185-87 (1999) "legal tether" standard that the conduct is "unfair" if it "violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law . . .," in that Plaintiffs' unfair prong is tethered to the violations of CFAA, ECPA, and CLRA, and to the underlying policies that led to the CCPA. As other courts have found, "This test is easily satisfied here because numerous California statutes—including the CCPA—'reflect 'California's public policy of protecting consumer data.' " *Brooks v. Thomson Reuters Corp.*, No. 21-CV-01418-EMC, 2021 WL 3621837, at *9 (N.D. Cal. Aug. 16, 2021) (citations omitted).

Finally, *Camacho v. Automobile Club of Southern California,* 142 Cal.App.4th 1394 (2006), initiates a third line of the "unfair prong" test and requires: "(1) The consumer injury must be substantial; (2) the injury must not be outweighed by any countervailing benefits to consumers or competition; and (3) it must be an injury that consumers themselves could not reasonably have avoided." *Id.; see also Daugherty v. American Honda Motor Co.*, 144 Cal.App.4th 824, 838-39 (2007). Here, Plaintiffs have alleged a substantial injury in that they have lost substantial amounts of money (FAC, ¶¶ 55-56); Apple has not identified any countervailing benefits resulting from it allowing "spoofing" application in the App Store; and Plaintiffs, who reasonably relied on Apple's long-standing campaign of "safety" could not have avoided injury.

[6] STATEMENT OF BASIS AND PURPOSE OF TRADE REGULATION RULE 408, UNFAIR OR DECEPTIVE ADVERTISING AND LABELING OF CIGARETTES IN RELATION TO THE HEALTH HAZARDS OF SMOKING, 29 Fed. Reg. 8355 (1964).

At the very least, the allegations are sufficient to raise factual issues that cannot be resolved at this early stage.

5. Damages are not an Adequate Substitute for Prospective Injunctive Relief

In arguing that Plaintiffs have "adequate remedies at law," Apple ignores Plaintiffs' requests for public injunctive relief, that Apple "be enjoined and restrained from distributing such 'phishing' or 'spoofing' applications in the App Store, and that this Court retain jurisdiction over this matter to monitor compliance with such an order." (FAC, ¶¶ 4, 75, 76, 98, 110, 113, 123). As numerous courts in this district have held, "monetary damages for past harm are an inadequate remedy for the future harm that an injunction under California consumer protection law is aimed at." *Zeiger v. WellPet LLC*, 526 F.Supp.3d 652, 687 (N.D. Cal. 2021); *see also Andino v. Apple, Inc.*, No. 2:20-CV-01628-JAM-AC, 2021 WL 1549667, at *5 (E.D. Cal. Apr. 20, 2021) ("*Sonner* does not warrant dismissal of his request for injunctive relief. Money damages are an inadequate remedy for future harm, as they will not prevent Defendant from continuing the allegedly deceptive practice.").

As monetary damages are not an "adequate remedy" for the prospective injunctive relief sought, needed so Plaintiffs (and the general public) can confidentially download cryptocurrency wallets going forward, Apple's "adequate remedy at law" argument fails.

And to the extent that Apple continues to assert that Plaintiffs' CLRA claim fails, there is no "adequate remedy at law." Nor do Plaintiffs need to allege that Apple *directly* acquired the stolen cryptocurrency. Plaintiffs merely need to allege that Apple "was unjustly enriched as a result of its allegedly unlawful business practices." *Cabebe v. Nissan of N. Am., Inc.*, No. 18-CV-00144-WHO, 2018 WL 5617732, at *6 (N.D. Cal. Oct. 26, 2018). The First Amended Complaint contains such allegations. (*See* FAC, ¶¶ 20-21). Either way, Apple's arguments fail.

H. Plaintiff Diep Has Alleged Violations of the Maryland Consumer Protection Act

Apple's arguments to dispose of Count IX, violations of the MCPA, again misconstrue the underlying allegations made by Plaintiff Diep. Plaintiff Diep did in fact allege that Apple

made misrepresentations to her as a consumer. (FAC, ¶ 146) (stating that Defendant intentionally . . . made representations and or omitted information about the App Store in general and thereby the Toast Plus application in specificity . . .which had or could have had the capacity, tendency, or effect of deceiving or misleading consumers."); (*See also Id*. ¶ 147, (similar); ¶ 148 (material omissions)).

Furthermore, Apple misrepresents to the Court the existence of a "reliance" requirement under the MCPA. Mot. at 21:1-20. Section 13-302 of the MCPA, "Deception or damage unnecessary," states, in full, that "[a]ny practice prohibited by this title is a violation of this title, whether or not any consumer in fact has been misled, deceived, or damaged as a result of that practice." Maryland Code Ann., Commercial Law, Art. § 13-302. While reliance may be needed to be plead in order to establish more than statutory damages, e.g., restitution, *see, e.g., Consumer Protection v. Consumer Pub.,* 304 Md. 731, 781 (1985), the clear language of the statute, the expression of the will of the elected officials of the General Assembly of Maryland, is not open to interpretation on this issue (and is not the issue the Defendants raise in the Motion).

Even if reliance needed to be pled, it was. Plaintiff states that "[t]hose statements, visual depictions, and failure(s) to state material fact(s) caused Plaintiff Diep and the Maryland Subclass to suffer pecuniary harm," (FAC, ¶ 150), a fair statement that the Plaintiff relied on the statements and omissions, and further, since the count incorporates all other preceding allegations, (*Id*. ¶ 146), all of the other allegations of reliance are incorporated into Count IX.

Just as the First Amended Complaint adequately alleges violations of the UCL and CLRA, it also adequately alleges a violation of the MCPA.

I. Plaintiffs Have Alleged Violations of the California Consumer Privacy Act

Apple's arguments to shield itself from liability under the California Consumer Privacy Act ignore both the law itself and underlying purpose of the statute. The CCPA's express intent is "to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information . . . in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control." Cal. Civ. Code § 1798.175. Consistent with this intent, the

statute provides that "[t]his title shall be liberally construed to effectuate its purposes." Cal. Civ. Code § 1798.194.

This purpose and intended construction provide guidance for interpreting the definition of the word "consumer," defined as "a natural person who is a California resident, *as defined in Section 17014 of Title 18 of the California Code of Regulations* . . ." Cal. Civ. Code § 1798.140(g) (emphasis added). The relevant California Franchise Tax Board definition makes clear that "resident" is defined as such to *include* those individuals that are "enjoying the benefit and protection of [California's] laws and government" and *exclude* those who "do not obtain the benefits accorded by the laws and Government of this State." 18 C.C.R. § 17014.

Here, Apple, via its Terms of Use, has imposed "the laws of the State of California" on the parties and has attempted to deprive them of the protection of any other jurisdiction. (Dkt. 43-3, 43-4, Terms § G). Having done so, the CCPA's liberal construction, and express intent of applying "the law that afford the greatest protection for the right of privacy for consumers," requires that the Plaintiffs (and the putative class) be treated as "residents," *i.e.* those that enjoy "the benefit and protection of [California's] laws and government."

Plaintiffs have also adequately alleged that Apple's security procedures are inadequate. As alleged in the First Amended Complaint, Apple has made an unqualified guarantee "that its App Store is 'a safe and trusted place'" (FAC, ¶¶ 2, 14-17, 102). The First Amended Complaint explicitly alleges that: (1) "Apple [authorized] a malicious application in the 'App Store' and [maintained] the same, despite knowledge of the criminal activity . . . " (*Id*. ¶ 1); (2) [D]espite numerous complaints regarding the fraudulent nature of the Toast Plus application, Apple allowed it to remain in the App Store and failed to warn Plaintiffs and Class Members of the danger of the application." (*Id*. ¶ 2); (3) At no time did Apple contact Plaintiff Diep to tell her that she had downloaded a malicious spoofing application (*Id*. ¶ 28); and (4) At no time did Apple contact Plaintiff Nagao to tell him that he had downloaded a malicious spoofing application. (*Id*. ¶ 33).

At this stage, such allegations are sufficient. *See Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, 2021 WL 6882377, at *5 (N.D. Cal. May 6, 2021) (denying motion to dismiss

CCPA claim based on "Plaintiffs' allegations that unauthorized third parties were able to access approximately 2,000 Robinhood customers' accounts and deplete their funds due to Robinhood's security measures are sufficient.").

And as Plaintiffs have lost substantial sums of money in reliance on Apple's assertions of "safety," any security procedures have proven inadequate. At the very least, Plaintiffs' allegation of harm resulting from the inadequacy of the security procedures create a reasonable inference in favor of Plaintiffs, sufficient to survive a motion to dismiss. *Cahill*, *supra*, 80 F.3d 336, 337-38.

J. Plaintiff Diep Has Alleged Violation of the Maryland Personal Information Protection Act That Are Actionable Under the Maryland Consumer Protection Act

Again, Apple misrepresents the allegations of Count VII in its Motion. While it is true that a violation of the Maryland Personal Information Protection Act ("PIPA"), Maryland Code Ann. Commercial Law, Section 14-3501, *et seq.*, is not a separate claim under Maryland law, Plaintiffs clearly stated in the Count that "[e]ach of the Defendant's failures under PIPA constitute violations of Maryland Code Annotated, Commercial Law, Title 13, the 'Consumer Protection Act' ('MCPA')." (FAC, ¶ 143). Because the issue here is Apple's failure to provide adequate security procedures and to notify consumers of the loss of their financial information, the allegations were pled as a separate count, to keep issues separate.

Second, Plaintiff did allege all the elements of a MCPA/PIPA claim. Specifically, Plaintiff alleged that she resides in Maryland, (FAC, ¶ 132), that "Defendant is a business that owns Personal Information of Plaintiff Diep and the Maryland Subclass Members," (*Id*. ¶ 133), that the Toast Plus application is a "phishing" or "spoofing" application, "one whose only purpose is to intercept financial information that was intended for another, legitimate recipient," (*Id*. ¶ 134), that "Defendant came to know of this illegitimate nature of the Toast Plus application some time before Plaintiff Diep became aware of her loss of private data," (*Id*. ¶ 135), "that this security breach included information that is considered Personal Information" under PIPA, (*Id*. ¶ 136), "that Plaintiff Diep's and Maryland Subclass Members' Personal Information was taken as a result of the distribution of the Toast Plus application," (*Id*. ¶ 137), that the "servers and

network connections in which the data breach occurred was controlled by Defendant," (*Id*. ¶ 138), that Defendant failed to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations," which was the direct cause of the data breach, (*Id*. ¶ 139), and that Defendant further failed to properly notify Plaintiff Diep and the Maryland Subclass Members of the unauthorized access of their Personal Information, as required by PIPA, in that no notice was given whatsoever. (*Id*. ¶ 141); *c.f.*, Mot. at 23:14-15 ("Diep has not alleged that Apple collected her personal information of that there was any breach of Apple's computer systems.").

Apple's reliance on *Johnson v. Baltimore, Police Dept.*, CV SAG-18-2375, 2021 WL 1610152, at *5 (D. Md. Apr. 23, 2021), is also misplaced. The *Johnson* case, to the extent relevant, considered a "survival" claim without statutory support. PIPA, however, expressly states that a violation of the Subtitle "[i]s an unfair or deceptive trade practice within the meaning of Title 13 of this article; and [ ] [i]s subject to the enforcement and penalty provisions contained in Title 13 of this article." Maryland Code Ann., Commercial Law, § 14-3508. The Motion must be denied as to Count VII.

K. <u>The Economic Loss Rule Does Not Bar Plaintiffs' Negligence Claim</u>

Apple's arguments regarding the "economic loss rule" are misplaced. To the extent that the economic loss rule applies to Plaintiffs' claims, the rule is wholly inapplicable because Plaintiffs seek damages beyond economic losses. As numerous courts in this district have held, the economic loss rule does not apply if damages beyond "pure economic loss" are sought. *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019); *see also Mehta v. Robinhood Fin. LLC*, 2021 WL 6882377, at *5 (N.D. Cal. May 6, 2021) (surveying cases).

Here, Plaintiffs have alleged loss of time as a harm. (*See e.g.* FAC, ¶¶ 55, 56; (*See also Id*. ¶¶ 57, 58, 73, 121, 157). This is enough to take the claims outside of the rule.

As to Apple's "duty," a merchant owes a duty to protect its customers from harm if it had actual or constructive notice of the condition and failed to remedy it "or have been able by the exercise of ordinary care to discover the condition, which if known to him, he should realize as

involving an unreasonable risk." *Ortega v. Kmart Corp.*, 26 Cal.4th 1200, 1206 (2001); *see also Ileto v. Glock, Inc.*, 349 F.3d 1191, 1203-4 (9th Cir. 2003).[7]

The First Amended Complaint alleges such a "duty," in that "[a]s a provider of goods and services through a near-monopolistic application market, Defendant has duties to consumers, *inter alia*, to take reasonable precautions to ensure that the goods it provides are reasonably safe and secure . . ." (FAC, ¶ 155).

Apple cannot magically make this basic duty disappear by asserting the existence of its "Terms." In fact, the case law cited by Apple does not support its position. *R.H. v. Los Gatos Union Sch. Dist.*, 33 F.Supp.3d 1138 (N.D. Cal. 2014), which was decided at the summary judgment stage (not the pleading stage), relates to injuries suffered during a school-sponsored wrestling match and the enforceability of an "'After School Sports Emergency/Health Insurance form' and *release*." *Id*. at 1145 (emphasis added). In making a *factual* determination, the *R.H.* court noted that "release agreements waiving liability for future gross negligence are unenforceable. . ." (*Id*. at 1168 (citation omitted)) and that "[a] liability release 'must be clear, unambiguous, and explicit in expressing the intent of the subscribing parties.' [citation] '[A] release must not be buried in a lengthy document, hidden among other verbiage, or so encumbered with other provisions as to be difficult to find.'" (*Id*. at 1166, citations omitted) . The determination made in *R.H.* cannot be made at the pleading stage. *See also* § V(B).

And even if the Court were to consider whether the hidden prolix in an extrinsic document has bearing on Apple's duty of care, Section G of Apple's Terms of Use do not contain the type of "release" language discussed in *R.H.* In fact, the word "release" does not appear anywhere in the section. (Dkt. 43-3, 43-4, Terms § G(f)). And a single paragraph buried in a 14-page document, assented to by "click-wrap" is not the type of "clear, unambiguous, and explicit" document anticipated by the *R.H.* court.

Regardless, courts in this District have rejected this exact argument in the past, finding:

[7] Apple's citation to *Diaz v. Intuit, Inc.*, No. 5:15-CV-01778-EJD, 2018 WL 2215790, at *5 (N.D. Cal. May 15, 2018) is entirely inapposite as that holding is limited to "noncustomers." In contrast to *Diaz*, here, the class is defined as users of App Store, *i.e.*, Apple's customers.

> [T]o the extent that Apple argues that it has no duty to review or evaluate apps and that it has disclaimed any liability arising from the actions of third parties, this argument both ignores contradictory statements made by Apple itself, and the allegations asserted by Plaintiffs regarding Apple's own conduct with respect to the alleged privacy violations. For one, it is not clear that Apple disclaimed all responsibility for privacy violations because, while Apple claimed not to have any liability or responsibility for any third party materials, websites or services, Apple also made affirmative representations that it takes precautions to protect consumer privacy. . . At the motion to dismiss stage, then, the Court is not prepared to rule that the Agreement establishes an absolute bar to Plaintiffs' claims."

In re iPhone Application Litig., 844 F.Supp.2d 1040, 1077.

Plaintiffs have also adequately alleged breaches of duty, in that, "Defendant breached those duties through act and omission, including, but not limited to, by failing to properly vet the Toast Plus application before providing it to the public, by failing to warn the public of the actual risks of applications in the App Store, by failing to remove Toast Plus from the App Store after learning of its dangerous nature, and or by failing to warn or notify each Toast Plus user of the danger after learning of the danger itself." (FAC, ¶ 156).

Having alleged a duty, breach thereof, and resulting harm, Plaintiffs have adequately alleged a claim for negligence.

VI. CONCLUSION

For the foregoing reasons, Apple's Motion should be denied.

Dated: June 6, 2022

CONN LAW, PC

/s/ Elliot Conn
Elliot Conn
Attorneys for Plaintiffs
HADONA DIEP, RYUMEI NAGAO
and the putative class